Revista de Marina Nº 959, pp. 34-39
ISSN 0034-8511

CIBERGUERRA...¿DUDÁIS?

Héctor Gómez Arriagada*

Resumen

Se presenta primero la visión de autores escépticos de la denominada ciberguerra, quienes señalan que no es más que una metáfora ilusoria. Se presentan luego argumentos que muestran como el tipo de guerra descrita por Clausewitz, se aleja de la forma en que los conflictos se están desarrollando en el siglo XXI. Para terminar, se fundamenta por qué las ciberoperaciones pueden ser un instrumento útil para la coerción.

Palabras clave: Ciberguerra; Clausewitz; ciberoperaciones; stuxnet.

Además del título de su última publicación en esta revista, Aramis (2016) dedica algunos párrafos a la ciberguerra señalando que el término responde a una mala traducción de *cyberwarfare*. Mientras que *war* corresponde a un término amplio que describe la condición de conflicto armado tal como en español lo hace la palabra guerra, cuando en inglés se le agrega la terminación *fare* puede denotar, por un lado, distintas tácticas y técnicas específicas que en su conjunto son metódicamente empleadas en el contexto de una guerra; o bien, referirse a un tipo de guerra de acuerdo a los métodos o tecnologías predominantes en la misma.

El término *nuclear warfare*; por ejemplo, se emplea para describir estrategias y tácticas que hacen empleo de armas nucleares durante una guerra, en el mismo sentido en que se emplea el término *naval warfare* para describir técnicas y tácticas para combatir en el medio marítimo. Por analogía *cyberwarfare* correspondería al conjunto de tácticas y técnicas específicas asociadas al empleo militar del ciberespacio.

Así entonces, cuando el término ciberguerra o guerra ciber es adoptado en el mismo sentido que guerra antiaérea, guerra de minas, guerra psicológica o guerra de guerrillas, el supuesto problema de la traducción no es tal y podría dejarse pasar por inocuo.

Es distinta la situación cuándo el término *warfare* es empleado para describir un tipo de guerra. Considerando que, por ejemplo, *conventional warfare* describe conflictos armados entre contendientes que no emplean armas nucleares, biológicas o químicas, se podría hacer un símil y señalar que *cyberwarfare* representaría un enfrentamiento bélico con énfasis en las operaciones en el ciberespacio, y desde esta perspectiva describiría un conflicto desarrollado principalmente en este dominio.

Y es en esto último donde subyace, en realidad, el cuestionamiento de fondo al término ciberguerra: ¿puede considerarse como guerra un enfrentamiento cuyas operaciones se desarrollan principalmente en el ciberespacio?, ¿pueden las ciberoperaciones realmente constituirse en un acto de fuerza que obligue a un adversario a acatar la voluntad de otro? (Clausewitz, 1832). Son estas algunas de las interrogantes que se espera responder en el presente artículo.

Visión escéptica

Uno de los principales argumentos de los escépticos de la ciberguerra es la visión

* Capitán de Navío. Magister en Ciencias Navales y Marítimas. Doctor en Comunicación y Magister en Ciencias de la Ingeniería Informática. (hgomez@ssffaa.gob.cl).

clausewitziana respecto de la naturaleza violenta de la guerra. Señala el estratega en su principal obra que la guerra implica el empleo de la fuerza física para desarmar al enemigo y, agrega, que el derramamiento de sangre y la brutalidad son elementos inseparables de ella. Pues bien, hasta ahora y por lo que se conoce, las operaciones en el ciberespacio están lejos de lo señalado por Clausewitz ya que la fuerza física estaría ausente en este tipo de acciones, no hay evidencia de muertes causadas directamente por un ciber ataque, ni menos se ha impuesto la voluntad de alguna de las partes con ciber operaciones.

Thomas Rid (2012) hace referencia a esto último cuando señala que las interacciones en el ciberespacio no son ni serán guerras, ya que las ciberoperaciones simplemente no son lo suficientemente letales para generar bajas significativas, por lo que nunca reemplazarán la violencia y, por lo mismo, están lejos de ser un acto de guerra; se agrega a lo planteado por Gartzke (2013) cuando señala que internet no será una alternativa ni sustituirá al campo de batalla.

Otros aspectos relevantes que estarían ausentes de las ciberoperaciones son la amenaza del uso de la fuerza y la disuasión, acciones que junto con explicitar la voluntad de empleo de un potencial bélico creíble, requieren que éste sea visible y evidencie su potencial de generar un daño inaceptable y, eventualmente, perdurable. ¿Cómo se hace esto en el ciberespacio?; pues es muy difícil porque las "ciber fuerzas" o "ciber unidades", aunque declaradas, no pueden ser comparadas o puestas a prueba ya que su eficacia depende, fundamentalmente del secreto de su potencial.

Desde la perspectiva de estos argumentos conservadores, es evidente que las actividades militares en el ciberespacio están lejos de constituirse, por sí solas, en un instrumento militar suficiente para imponer la voluntad sobre un adversario y; en términos de gran estrategia, la ciberguerra no podría constituirse en un tipo de guerra ya que en síntesis -y siempre desde la visión clausewitsiana-, no sería violenta ni letal.

Otro argumento contundente para desacreditar el término ciberguerra viene de la lingüística, especialmente cuando se descubre que la palabra en sí no es más que una metáfora empleada en su momento, para describir fácilmente eventuales efectos adversos de la conectividad, la posibilidad de explotación de las vulnerabilidades de sistemas de información con fines maliciosos por parte de terceros y lo relevante que resulta tomar medidas de seguridad para protegerlos.

Lawson (2012) señala que al haberse aplicado a las actividades maliciosas en el ciberespacio la metáfora de la guerra, se inició una serie de vinculaciones que han llevado a institucionalizar no sólo el término ciberguerra, sino que además ha generado toda una cultura alrededor capaz de esbozar estrategias militares *ad hoc*, crear cibercomandos, generar iniciativas para transformar internet e incorporar en el derecho internacional conceptos para equiparar un ciberataque con los ataques físicos.

Es más, se ha planteado que esta realidad creada por un lenguaje militarista es peligrosa, ya que justificaría escalar innecesariamente un conflicto hacia acciones violentas en base a supuestos actos de guerra que no lo son (Dunn, 2011). Esto además se confabula con el proceso de securitization[1] al que se ha sometido la ciberseguridad en los últimos años, así como con el sensacionalismo de la prensa y la aprobación cómplice de la industria de la ciberdefensa.

¡Pero la guerra evoluciona!

Pero utilizar el marco teórico dado por Clausewitz para descartar la ciberguerra parece un ejercicio simplista ya que, después de todo, basta con señalar como ésta no se encuadra en aquel marco desarrollado en 1832 a la sombra de las guerras europeas de los siglos XVIII y XIX. Sin embargo y a pesar de la veneración por este autor, desde finales de la guerra fría se inició un intenso debate entre detractores y adherentes respecto de la pertinencia de aplicar la tesis del prusiano en los conflictos contemporáneos.

Por un lado, sus críticos señalan que no sólo su fundamental trinidad de la guerra es obsoleta, sino que sus afirmaciones respecto a la tendencia a

1. Teoría de las relaciones internacionales de Ole Waever que describe el proceso por el cual los actores de un Estado, a través del discurso, transforman un asunto cualquiera en relevante para la seguridad nacional, con el fin de legitimar medidas extraordinarias (como restricción a las libertades, movimientos militares o asignación de recursos extraordinarios) usando como argumento la necesidad de enfrentar la supuesta amenaza que dicho asunto representa.

la violencia descontrolada, la racionalidad de los objetivos políticos de los Estados, el protagonismo de éstos y el enfrentamiento entre fuerzas armadas estatales de la misma naturaleza, son en la actualidad una falacia producto del desarrollo social, la debilitación de la influencia de los Estados en un mundo globalizado y la aparición de actores no estatales en los conflictos.

Sus defensores, por otra parte, alegan que Clausewitz advierte que la guerra cambia su apariencia según el caso, y que no desconoce que las características de cada época pueden tener un impacto tanto en los objetivos como en los métodos de la guerra; por lo mismo, sus apóstoles arguyen que, reinterpretados, los principios planteados en su principal obra son perennes y pueden aplicarse perfectamente a las denominadas nuevas formas de la guerra contemporánea.

En términos generales, las nuevas guerras se caracterizarían por su absoluto alejamiento de la visión de Clausewitz de un enfrentamiento entre Estados, con una separación difusa entre combatientes regulares e irregulares, así como de la población civil la que, a su vez, estaría mucho más comprometida en las acciones de combate ya sea como blanco o como combatiente. En la mayoría de los casos la tradicional secuencia de una paz seguida de acciones de combate, que finaliza con un claro ganador del conflicto, se ha reemplazado por conflictos inconclusos los cuales, aun agotados, no necesariamente satisfacen objetivos políticos ni tampoco erigen vencedores claros.

El modelo de las guerras de cuarta generación, por ejemplo, considera que las guerras contemporáneas típicas son las que antes se conocían como no convencionales, y en las cuales los actores emplean medios diversos como militares, económicos, sociales o políticos; no diferencian entre civiles o militares ni tampoco entre situación de paz o guerra (Singh, 2005). Los desarrolladores del concepto consideran que la idea clausewitziana de buscar y destruir las fuerzas principales adversarias en una gran batalla decisiva, es un concepto de las guerras de segunda generación -caracterizadas por la capacidad de aplicar poder de fuego de manera masiva y en movimiento- táctica muy distinta a la no lineal de la guerra de maniobras de tercera generación, agregando que las de cuarta generación enfatizarán a nivel operacional y estratégico la supremacía tecnológica, las operaciones sicológicas y las intervenciones de información y medios (Lind, Nightengale, Schmitt, Sutton y Wilson; 1989).

El concepto de operaciones basadas en efectos, por otro lado, considera que no siempre es necesario el desgaste o aniquilación de las fuerzas adversarias, ya que en ocasiones se pueden lograr los mismos efectos por medios directos, indirectos y acumulativos usando instrumentos militares, diplomáticos, psicológicos y económicos. El concepto considera la complementación de las operaciones destructivas, de ocupación, disrupción y desgaste con armamento de alta precisión y operaciones en el ciberespacio (Davis, 2001).

El general Rupert Smith (2007), por su parte, señala que simplemente ya no existen las guerras entendidas como un enfrentamiento entre Estados, desarrolladas en campos de batalla en los que se enfrentan fuerzas armadas que buscan destruirse entre sí. En cambio, éstas han sido reemplazadas por las que denomina guerras entre pueblos (*war amongst the people*) de naturaleza eminentemente asimétrica, en las cuales la distinción entre combatientes y no combatientes se ha vuelto difusa y los campos de batallas incluyen civiles; guerras en las que los objetivos físicos se reemplazan por efectos deseados blandos, que no necesariamente se alcanzan con la aplicación de la fuerza militar, sino que también con medios para influenciar audiencias propias o adversarias, civiles o militares.

El paradigma de las nuevas guerras (*new wars*) de Mary Kaldor (2013) indica que en ellas la condición de violencia organizada ya no es monopolio de los Estados, puesto que en éstas intervienen conjuntos o redes de Estados que entregan soberanía, o bien, actores no estatales; sus fines más que motivados por intereses políticos o ideológicos, lo están por la identidad étnica, tribal o religiosa. En cuanto a los métodos, señala que la conquista de territorio se hará efectiva por medio del control de la población y que la violencia será principalmente dirigida a los civiles, afirmando que este nuevo tipo de guerras tenderán a expandirse en un estado de conflicto continuo.

Martin van Creveld (2008) señalaba que para el año 2010 los grandes conflictos armados entre Estados constituirían una excepción, entre otras razones, por la proliferación nuclear, el cambio de actitud hacia los conflictos armados, la inaceptabilidad de enfrentamientos bélicos con fines de conquista de territorios, sus costos y el aumento de la interdependencia. Agrega que a la luz de los conflictos contemporáneos, la visión trinitaria de la guerra de Clausewitz en nada encaja con la mayoría de los enfrentamientos bélicos posteriores a la Segunda Guerra Mundial, señalando que casi todos ellos adoptaron la forma de guerras asimétricas, guerrillas, insurgencia, guerras incendiarias, de baja intensidad, guerras no lineales o híbridas; todos nombres dados a las que él identifica como guerras irregulares.

Por otro lado, hay casos que muestran que esta transformación también se ha evidenciado en algunos de los pocos conflictos interestatales posteriores al término de la guerra fría. En un informe del Colegio de Defensa de la OTAN, Can Kasapoglu (2015) señala que después de la guerra entre Georgia y Rusia en 2008, este último país ha mostrado una evolución tendiente al desarrollo de una guerra no lineal centrada en la penetración del adversario. Destaca que particularmente en su conflicto con Ucrania por la anexión de Crimea, los rusos han combinado dos antiguos conceptos soviéticos: las teorías de operación en profundidad y control reflexivo.

Mientras la primera busca la penetración profunda del aparato militar, la inteligencia y las operaciones de información del enemigo, evitando un enfrentamiento armado convencional; la segunda, espera hacer actuar al adversario de una manera conveniente usando métodos sistemáticos para condicionar sus percepciones. Señala que tanto a nivel estratégico como operacional y táctico, la doctrina rusa enfatiza el rol de los medios no militares, la manipulación a través de la desinformación, las fuerzas especiales y la reducción de los factores de fricción.

A la luz de estas nuevas visiones y sus fundamentos, parece insensato sostener que un modelo teórico elaborado para comprender las guerras europeas hasta el siglo XIX sea aplicable a toda época y circunstancia; ¡más aún para desechar el surgimiento de una forma de conflicto propia del siglo XXI! Es decir, siendo una realidad que las guerras han cambiado desde el siglo XIX, las hipótesis entonces aceptadas necesitan ser verificadas y, si es necesario, modificadas (Shepard, 1990). Este es un cuestionamiento aplicable a estrategia, táctica, doctrina y principios; no hacerlo implica el riesgo de aferrarse porfiadamente a un dogma y mantenerlo con tenacidad y dureza a pesar que puede estar errado u obsoleto.

Pero a pesar de las críticas a Clausewitz, uno de los elementos constitutivos de la guerra descritos por él y que no ha sido cuestionado, es el rol que juega la violencia o la amenaza de su empleo. Por lo mismo, e independiente del marco teórico empleado, para determinar si las acciones en el ciberespacio pueden constituir un instrumento de coerción, es necesario establecer si las mismas tienen el potencial de infringir sufrimiento, causar daños permanentes o, al menos, si pueden considerarse violentas.

Ciberguerra

Ya sea en el modelo clausewitziano como en cualquiera que adhiera a las nuevas guerras, la violencia o el uso de la fuerza se ha relacionado con el empleo de algún mecanismo diseñado específicamente para dañar vidas humanas, estructuras o sistemas: armas. Mucho se ha discutido respecto de si las ciberoperaciones tienen precisamente este potencial, como condición *sine qua non* para considerarlas una acción armada y, por extensión, fundamentar las afirmaciones que indican que las ciberoperaciones sí pueden constituirse en un instrumento de la fuerza militar para la coerción y el desgaste.

Schmitt (1999) luego de un interesante análisis del marco normativo que regula las relaciones internacionales, precisa que las acciones ofensivas en el ciberespacio denominadas *computer network attack* pueden considerarse como un acto de coerción, que pasan a constituirse en uso de la fuerza cuando tienen el propósito de causar daño o disrupción, y se transforman en ataque armado si sus consecuencias son daños a la infraestructura o heridas a las personas.

Agrega Schmitt que en base a la práctica de las relaciones internacionales las consecuencias indicadas deberían ser, además, severas, inmediatas

y verificables; especificando que constituirían un acto de guerra con derecho a respuesta, si el ataque es perpetrado por unidades militares, forman parte de una operación que incluirá acciones cinéticas o sus efectos son evidentes en el país atacado. Finaliza señalando que cuando una operación a través del ciberespacio no cumple las condiciones para considerarla ataque armado o un uso de la fuerza, al menos podría asociarse a una intervención en los asuntos internos de otro Estado.

Está claro que una aproximación basada en los efectos finales da mucho más soporte al concepto de ciberguerra. En esta línea, Lewis (2011) plantea como ejemplo que una denegación de servicios que interrumpa la operación de los mismos de un puerto importante de un país afectando su comercio internacional, puede considerarse un ataque porque sus efectos serían equivalentes al de un bloqueo naval. Por su parte, Applegate (2013) señala que en la actualidad hay evidencia empírica que demuestra que los ataques a través del ciberespacio sí pueden tener efectos físicos.

Entre otros ejemplos menciona el proyecto Aurora, un experimento en el año 2007 del *Department of Homeland Security* de EE.UU. por medio del cual un atacante fundió un generador eléctrico por la intervención remota de su sistema de control; además, menciona otras pruebas y validaciones teóricas que van desde la toma de control de vehículos, hasta la alteración del funcionamiento de dispositivos médicos implantados en pacientes. En cuanto a experiencias reales, menciona intervenciones remotas a diferentes sistemas de control que causaron inundaciones en Australia, alteraciones al control de tránsito en Los Ángeles y el choque entre tranvías en Polonia incidente que, dicho de paso, describe como el primer caso documentado de un ciberataque que causa heridos.

En cuanto a experiencias operacionales bastante se ha escrito de Stuxnet, el que sería el primer caso de una ciberarma diseñada específicamente para causar daños físicos (Frederick, 2016). Por su parte Clarke (2009) señala que entre las misiones del *US Cyber Command*, está lanzar ataques a través del ciberespacio para generar efectos físicos en instalaciones e infraestructura, en especial en los sistemas de defensa aérea, eléctricos, comunicaciones, etc.

Se puede señalar entonces que a través del ciberespacio sí son posibles tanto las manifestaciones de violencia entre Estados, como el uso de la fuerza, los ataques armados y los actos de guerra; es más, pueden tener efectos en la infraestructura física y el potencial de causar heridos y eventualmente la muerte de personas. Se puede afirmar que aunque su potencial destructivo en la actualidad es aún incipiente y muy limitado, la ciberguerra es una realidad y se prevé que tanto su empleo como sus efectos físicos se irán incrementando con el tiempo.

Conclusiones

Restringir la comprensión del conflicto en general y de la guerra en particular al marco teórico de Clausewitz desarrollado hace más de 170 años, implica limitar el pensamiento crítico respecto de un asunto que tiene en la actualidad innumerables variaciones. De hecho, existen diferentes teorías que señalan que es necesario replantearse la concepción de guerra, violencia, acto de guerra, ataque armado y uso de la fuerza, en especial los esbozados por el prusiano.

En el ciberespacio son posibles las manifestaciones de violencia con el potencial de causar daños físicos, heridos y muertos, lo que se prevé irá en aumento.

Y aún cuando el potencial destructivo de las ciberoperaciones es marginal por ahora, pueden considerarse un instrumento valioso en el contexto de los denominados conflictos irregulares o de baja intensidad, en las crisis o en los enfrentamientos políticos entre Estados.

Dada su todavía limitada capacidad de generar daño en comparación con las denominadas armas cinéticas, a la fecha el campo más provechoso para las ciberoperaciones está en el sabotaje y el espionaje.

Ciber…¿guerra?; sí, ciberguerra.

* * *

BIBLIOGRAFÍA

1. Applegate, S. (2013).The dawn of kinetic cyber.5th International conference on cyber conflict, NATO CCD COE Publications, Tallin.Obtenido en Diciembre 2016 en https://ccdcoe.org/cycon/2013/proceedings/d2r1s4_applegate.pdf
2. Aramis.(2016). Las tertulias tácticas de Acapulco y el Alemán.Ciber... ¿guerra?Revista de Marina; 133/950, Ene/Feb pp. 92-95.Obtenido en Octubre 2016 en http://revistamarina.cl/revistas/2016/1/aramis.pdf
3. Clarke, R. (2009). War from cyberspace.The National Interest, November/December.Obtenido en Diciembre 2016 en http://users.clas.ufl.edu/zselden/coursereading2011/Clarkecyber.pdf
4. Clausewitz, C. (1832). De la Guerra. Berlín.Obtenido en Septiembre 2016 en http://lahaine.org/amauta/b2-img/Clausewitz%20Karl%20von%20-%20De%20la%20guerra.pdf
5. Davis, Paul. (2001). Effects-Based operations.Office of the Secretary of Defense and the United States Air Force.Rand Corporation. Obtenido en Diciembre 2016 de http://www.rand.org/content/dam/rand/pubs/monograph_reports/2006/MR1477.pdf
6. Dunn, M. (2011).As likely as visit from E.T. European Magazine (N°7, January).Obtenido en Diciembre 2016 de http://www.theeuropean-magazine.com/myriam-dunn-cavelty--2/6128-cyberwar-and-cyberfear.
7. Frederick, E. (2016). Stuxnet, la primera ciberarma. Revista Marina N°133/951, Mar/Abr.Obtenido en Noviembre 2016 en http://revistamarina.cl/revistas/2016/2/efrederickr.pdf
8. Gartzke, Erik. (2013). The Myth of Cyberwar: Bringing War in CyberspaceBack Down to Earth. International Security, Vol. 38, No. 2 (Fall 2013), pp. 41–73, doi:10.1162/ISEC_a_00136.
9. Kaldor, M. (2013).In defence of new wars.Stability, 2(1): 4, pp. 1-16. DOI:http://dx.doi.org/10.5334/sta.at
10. Kasapoglu, C. (2015). Russia´s renewed military thinking: Non-linear warfare and reflexive control. Research paper N°121, November. Research Division, Nato Defense College. Rome.Obtenido en Octubre 2016 en http://www.ndc.nato.int/news/news.php?icode=877
11. Lawson, S. (2012). Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States.FirstMonday, Volumen 17, N°7.Obtenido en Septiembre 2016 en http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270
12. Lewis, J. (2011). Cyberwar thresholds and effects.IEEE Security & Privacy.Volume: 9, Issue: 5, Sept.-Oct. Obtenido en Octubre 2016 en https://www.researchgate.net/publication/220497024_Cyberwar_Thresholds_and_Effects
13. Lind, W.; Nightengale, K.; Schmitt, J.; Sutton, J.; y Wilson, G. (1989).The changingface of war: into the fourth generation. Military Review, October. Obtenido en Noviembre 2016 en https://www.mca-marines.org/files/The%20Changing%20Face%20of%20War%20-%20Into%20the%20Fourth%20Generation.pdf
14. Rid, T. (2012). Cyber war will not take place. The Journal of Strategic Studies Vol. 35, No. 1, 5–32.http://dx.doi.org/10.1080/01402390.2011.608939.ObtenidoenDiciembre 2016
15. Shepard, J. (1990). On war: Is Clausewitz still relevant? Parameters, Sept. US Army War College.Obtenido en Septiembre 2016 en https://www.researchgate.net/publication/235143713_On_War_Is_Clausewitz_Still_Relevant
16. Singh, G. (2005). Fourth generation war: paradigm for Change (Thesis). Naval Post GraduateSchool. Obtenido en Dicimbre 2016 en http://www.dtic.mil/dtic/tr/fulltext/u2/a435502.pdf
17. Schmitt, M. (1999). Computer network attack and the use of force in international law: thoughts on a normative framework. Institute for information technology applications, USAF Academy.Obtenido en Diciembre 2016 en www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471993
18. Smith, R. (2006). Interview with General Sir Rupert Smith.International Review of the Red Cross.Volume 88, number 864, December. Obtenido en Diciembre 2016 en https://www.icrc.org/eng/assets/files/other/irrc_864_interview_rupert_smith.pdf
19. Van Creveld, M. (2008). The transformation of war revisited. Small wars & insurgencies, 13:2, 3-15, DOI: 10.1080/09592310208559177